“Privacy Management: The Privacy Profession in the Public and Private Sectors”

Testimony of Kirk M. Herath
Chief Privacy Officer, AVP-Associate General Counsel,
Nationwide Insurance Companies
and
President, International Association of Privacy Professionals

Before the United States House of Representatives
Committee on Homeland Security,
Subcommittee on Intelligence, Information Sharing
and Terrorism Risk Assessment

April 6, 2006

Introduction

Mr. Chairman, members of the Subcommittee good morning. Thank you for opportunity to speak with you this morning.

My name is Kirk Herath, I am the Chief Privacy Officer, Associate Vice President, and Associate General Counsel for Nationwide Insurance Companies, located in Columbus, Ohio. I am also currently serving as President of the International Association of Privacy Professionals (IAPP), the world's largest association for the privacy field, representing over 2,000 privacy professionals in business, government, and academia from 23 countries. Additionally, I serve as a member of the Department of Homeland Security's (DHS) Data Privacy and Integrity Advisory Committee, which advises the Secretary of the Department of Homeland Security and the DHS Chief Privacy Officer on privacy and data integrity issues related to personal information.

I would like it noted that I am here today in a personal capacity as an expert in privacy and privacy compliance. I am not here today officially representing my employer, my professional association or the Data Privacy and Integrity Advisory Committee. Thus, the opinions expressed here are mine alone and do not reflect those of any other person or organization.

This morning, I will explain to the Committee how privacy has become imbedded into most private and a growing number of public organizations and how, in fact, it has become a legitimate profession and career path for thousands of knowledge workers. I also will attempt to describe for the Committee the very basic steps any organization needs to go through to address privacy and build a privacy infrastructure. Following this description, I will compare and contrast the role that the DHS Privacy Office plays to what any other privacy office would do, whether it is private or public sector, particularly the trade-offs and balancing that is required to be successful. Finally, I will also respectfully attempt to provide a brief set of recommendations for the Committee to consider if it desires to ensure more consistent privacy protections for DHS, or for any federal agency that collects and processes personal information.

The Profession and Business of Privacy

Before I describe how privacy programs should be organized and compare that to the DHS Privacy Office, I would like to discuss profession of privacy and the work of the IAPP. I believe that this will provide a good framework for the Subcommittee to see how Privacy is a vibrant and growing profession. In sum, privacy is recognized by the private sector, and increasingly in the public sector and academia, as an important and integral part of an organization's success. The growth of the IAPP reflects this view. The IAPP is a rapidly growing professional association that represents individual members working in the field of privacy. The organization works to define and promote this nascent profession through education, networking, and certification.

In many ways, the emergence and growth of the IAPP reflects the growing importance of privacy in public and private sectors. Privacy protections within the government and marketplace require professionals to assess, create, monitor, and maintain policies and practices. Put simply: privacy professionals are needed to give privacy protections viability within any organization.

The IAPP was founded five short years ago as an emerging network of privacy professionals recognized the need for a professional association. The organization has grown rapidly since those early days and now boasts over 2200 members in 23 countries. The IAPP's recent annual conference here in Washington was, to the best of my knowledge, one of the largest privacy conferences ever held, with over 800 attendees. Clearly, the market has placed a very high value on privacy and the robust, but responsible use of data.

When the IAPP was initially formed, the majority of our members shared a similar title: chief privacy officer, or CPO. Indeed, many – if not most – Fortune 500 companies have now appointed a chief privacy officer. But the majority of IAPP members are not CPOs. Rather, we have seen a robust hierarchy of professional roles in privacy emerge – in both the privacy and the public sectors. These privacy pros cover issues of compliance, product development, marketing, security, human resources, consumer response, and more. The management of privacy issues in large organizations now requires a broad and deep team of professionals with increasingly sophisticated skills. It is a hybrid profession encompassing a broad set of skills. Some organizations have even created job families for their privacy professionals. It is now a career track.

The job of a privacy professional demands mastery of a complex set of laws, technology, security standards, and program management techniques. In 2004, the IAPP introduced the first broad-based privacy certification to the US marketplace, the Certified Information Privacy Professional (CIPP). This credential is meant to serve as a demonstration of a candidate's knowledge of a broad range of fundamental privacy concepts. To date, over 800 people have taken the exam and over 600 CIPPs have been granted in the US.

In 2005, the IAPP extended the CIPP program to include issues of governmental privacy. The CIPP/G program covers issues specific to the public sector: such as the Privacy Act, eGovernment Act, Freedom of Information Act, Patriot Act, and more. To date, the IAPP has granted over 70 CIPP/Gs. The IAPP expects more growth in this sector, due to the growing importance of privacy in the public sector. This hearing reinforces that view.

Clearly, the profession of privacy has cemented its position as a critical resource in any organization that deals with data – whether that data is consumer or citizen data, or both. Privacy professionals within DHS and the few other government agencies that have privacy offices play an important role in further our nation's twin goal of protecting its citizen's security and their rights.

I encourage members of the committee to visit the IAPP's website, www.privacyassociation.org, to learn more about the profession of privacy. And, as a CIPP/G myself, I strongly recommend that the committee consider the value of such privacy certifications as a tool to ensure privacy issues are properly identified and addressed in the public and private sectors.

Operationalizing Privacy within an Organization – An Example

One of the reasons Chairman Simmons invited me today was to provide the Committee with a brief overview of the process private sector companies undergo to implement an effective privacy program. I believe that the steps taken by private sector companies take to protect the privacy of personal information can easily be extrapolated to the public sector. To the best of my knowledge, these were essentially the same steps that the DHS Privacy Office completed in order to provide the same privacy protection that individuals have come to expect from all entities that collect, use, and share their personal information.

I will use my own experience with Nationwide to describe for the Committee the basic steps necessary for any organization – either public or private – to implement and continue to manage its privacy responsibilities. Explaining how privacy has been adopted in the private sector will help illustrate the steps – including opportunities and challenges – necessary to effectively carry out a privacy program.

First, let me give you a brief overview of Nationwide. Nationwide is a fortune 100 company comprised of several dozen different companies and divisions that sell a variety of products – from auto, home, and commercial insurance to mortgages to financial products – such as annuities and investment funds, to retirement plans – such as 401k and 457 plans. Nationwide employees over 30,000 employees and has an exclusive sales force of just over 4,000 agents. It also sells its products and services through tens of thousands of independent agents, producers and brokers. Despite a complex organization, we have a legal duty to safeguard our customer information and protect their data wherever it is stored, accessed or shared. This can be a daunting task without a good plan and organization.

Nationwide began centrally managing privacy as Congress was putting the finishing touches on the Gramm-Leach-Bliley Act (GLBA) in late 1999. As you may know, GLBA requires financial institutions, including banks and insurance companies, to inform customers in an annual privacy statement how the company uses, protects, and shares customers nonpublic personal information. GLBA also requires that financial institutions safeguard customer information. It's not enough for a company just to tell a customer that it is "protecting your nonpublic personal information" or that "access to your information is limited to employees who have a business need-to-know your information." A company must have the processes and technological controls in place to veritably support the privacy statement.

Prior to GLBA, each entity of Nationwide managed compliance with state privacy laws – mainly some version of the 1982 Model National Association of Insurance Commissioners (NAIC) Privacy Act – independently in the 16 states where some version of this model had been enacted into law. To the extent possible, each company or division managed privacy practices differently. As you can imagine, this created a patchwork effect with respect to privacy. Each company and division adopted different privacy standards and practices. Even the philosophy of privacy varied between companies, with some companies following a very high standard for privacy and others following a standard that was the minimum necessary to comply with the law. Senior management had not articulated a uniform privacy policy and spread this policy throughout the organization, companies and divisions. In sum, there was no consistent guidance on privacy. To be fair, this situation existed because there was no single set of national privacy laws that applied equally to every entity, and there was no real enforcement mechanism.

For the private sector, this all changed when Congress enacted the Gramm-Leach-Bliley Act in November 1999. Among other requirements, the GLBA effectively forced companies to centralize privacy management and compliance. The sheer scale of implementing the privacy and safeguard requirements of GLBA required a centrally coordinated office to coordinate the implementation of one corporate privacy policy that complied with the new set of laws. I was assigned the role of advising Nationwide executive leadership on a privacy policy and compliance plan and then, with their agreement and approval with this privacy policy and plan, to implement GLBA requirements throughout all Nationwide companies and divisions.

GLBA and other federal and state privacy laws have had a positive effect on customers and citizens. A good example of this is that DHS probably would not have hired the first statutorily-required privacy officer in the federal government, Nuala O'Conner Kelly, if not directed to do so by law. Customers and citizens have come to expect that entities that use, share, or disclose their personal information should protect this information and should use, share, or disclose it appropriately. The federal government appears to be coming to the same conclusion: a central office is needed to coordinate privacy for any large government agency, perhaps one is even needed to coordinate "among" the federal agencies, but I will address that later.

The Four Basic Steps of a Privacy Program

One can find several books and a plethora of articles today about how to create a privacy program. Most of these are good descriptions that go into each area in great detail and are worthwhile reading. However, the steps in creating a privacy program can be summed up in the following manner. To implement a privacy program, any company or agency needs to follow a seemingly simple four step model:

1. Assess,
2. Address,
3. Monitor and Audit,

4. Repeat.

Step One – Assess

The goal in step one is to conduct dozens and dozens of assessments. The best way to carry out this task is to create a large cross-functional team. For example, in my case, I formed what we called a Virtual Privacy Team (VPT) that included about 40 people from across our corporation. Each Nationwide company or division had representation on the VPT. These team members in turn lead their own business unit or staff office privacy compliance team, which varied in size and scope, within each of the companies or divisions. By my estimation – by using this model, we were able to centrally manage and coordinate the activities of over 500 employees actively working on our corporate privacy implementation during 2000-2001, which was the high water compliance year of us, as we worked to comply with strict legal and regulatory time lines.

Basically, the objective in the first step in implementing privacy in an organization is to assess current processes, procedures, uses of data, etc. Any organization going through this process needs to conduct, among others, the following assessments:

1. Analysis of the legal requirements.

    a. What federal or state privacy laws exist that affect the organization?
    b. What were the specific requirements for each privacy law?
    c. How were companies and divisions complying with these patchwork of regulations?

2. Evaluation of existing privacy standards, practices, and philosophies.

3. Evaluation of information security practices.

    a. Does Nationwide have an information security policy?
    b. Does it meet the standards of the Safeguard Rule (the companion information security regulation within GLBA)?
    c. Collection of personal information.
    d. Which areas of Nationwide are collecting personal information?
    e. What type of information is being collected?
    f. Why is this type of information being collected (purpose)?
    g. Where is it stored?
    h. Is Nationwide only collecting personal information necessary to complete the customer's request?

4. Collection of Personal Information.
    a. Which areas of Nationwide are collecting personal information?
    b. What types of information is being collected?
    c. Why is this type of information being collected (purpose)?

d. Where is it stored?
e. Is Nationwide only collecting personal information necessary to complete the customer's request?

5. Use of Personal Information.

    a. How is information being use?
    b. What is it being used to accomplish for the organization?
    c. Is there a legal or rational basis for each use of information?

6. Access to Personal Information.

    a. Who can access personal information?
    b. Does everyone with access have a business need-to-know the information?
    c. Is access monitored?
    d. Are employees technologically capable of accessing personal information that they should not be able to access?

7. Disclosure of Personal Information

    a. How is personal information shared within Nationwide?
    b. Are the principles of need-to-know enforced?
    c. Do these disclosures have a legal basis?

8. Disclosure of Personal Information with Third Parties.

    a. Does a contract exist with all third parties that receive Nationwide information?
    b. Have we conducted an information security audit to determine whether the third party is capable of adhering to the laws that require the information to be protected?

9. Data Integrity

    a. Is the data accurate and up-to-date?
    b. Is there a way for customers to access their data and valid correct errors?

10. Management

    a. What documentation or privacy procedures exist?
    b. Is it up-to-date, accurate, and sufficient for the company of division?
    c. Does it need to change to satisfy the new law?
    d. Can it be extrapolated to the rest of the organization as a best practice?
    e. Is there anyone responsible for complying with laws and regulations?

After going through the first assessment, which formed our legal analysis of privacy, the VPT in conjunction with a steering committee that I chaired drafted a privacy policy for Nationwide and a privacy statement detailing our privacy policy for our customers. The privacy policy was then adopted by a steering committee of senior Nationwide executives. This became the privacy philosophy that the VPT adhered to when implementing privacy across all Nationwide companies and divisions. It was the foundation upon which we have built our program over these past six years.

Step Two – Assess

Over an 18-month period, as these different assessments were completed, the VPT concurrently analyzed the results and determined how they fit with the overarching privacy policy. We then addressed the key question of whether the results of the assessment were sufficient or did they need modifications to match the newly drafted privacy policy? This is the hallmark of step two, which is identify and address gaps in your processes and procedures.

In step two, the VPT and small number of outside consultants conducted gap analyses between the legal requirements, the new Nationwide Privacy Policy and the results of the different assessments. For example, number nine in the assessment list, above, was Disclosure of Personal Information with Third Parties. To address this assessment, the VPT member worked with the team responsible for executing contracts in each company or division to evaluate the findings in the assessment against the legal requirements and Nationwide's Privacy Policy. In some cases, they discovered that they could not find a copy of a contract, or that a written contract didn't exist. Many contracts did not contain the new confidentiality, privacy, and information security, language required by the GLBA. These teams identified the gaps and developed a plan to address the gaps identified.

The VPT then created project plans to address the gaps. Let's use an assessment from earlier – Access to Personal Information. One of the items of the assessment was an illustration of how personal information flowed through a company or division. This assessment included where the personal information was stored and which associates could access it.

The privacy sub-team then documented the tasks necessary to address the gap between the assessment and both the legal requirements and Nationwide Privacy Policy. The next step was to develop a project plan to assign the activities for each task and to monitor the progress.

Step Three – Monitor and Audit

After the dozens and dozens of projects to address the identified gaps were finished, we created a privacy compliance program to audit the privacy procedures that the teams implemented. For practical reasons, this program was created and housed in the Office

of Privacy, because it contained the evolving set of experienced professionals capable of carrying out these tasks.

There are several purposes to the audit phase of privacy implementation. One purpose is to confirm that the privacy processes are still operating. Sometimes, when the novelty of a project fades, employees inadvertently regress back to old practices. Also, employees often change jobs and the institutional memory leaves the unit. Monitoring through self-assessment or more formal audits keep compliance issues fresh and illustrate actual privacy practices to business leaders.

Another purpose of continuous monitoring or auditing is to determine whether a compliance process change is necessary as a result of a new business process. Business is a constantly changing environment. Audits help discover when new privacy processes are necessary to meet these new changes.

Finally, informal monitoring and audits prepare companies for formal market conduct audits by regulators. Regularly conducting internal audits allows business to understand and address privacy risks before a regulator conducts an audit. This reduces the risk of regulatory enforcement and fines.

Step Four – Repeat

Privacy implementation never ends. Thus, the four step process is really a continuous improvement loop. This has been extremely important over the past six years, as each year the private sector has been faced with an ever expanding array of legislative and regulatory requirements around privacy and information security. In addition to the changing legal landscape, a company is required to repeat the process to accommodate new business goals or changes to existing processes.

In summary, this may be an overly simplistic explanation of the complex process of implementing privacy throughout any organization – public or private.
However, I believe that it correctly points out the nature of the process and is easy to understand. There is one other important item to note here. None of this is possible without a clear mandate and strong support from the top of the organization. If the privacy office lacks the support of the chief executive, whether this is a private or public organization, it will never be able to effectively carry out its mission. A privacy office without senior management support may be worse than not having a privacy office, because it merely provides an illusion of privacy without the reality.

The Challenges – Balancing Competing Interests

Earlier, I discuss the requirement for financial institutions to create a privacy statement, which describes how the company uses, protects, and shares customer information. It is difficult for a large company like Nationwide to make blanket promises to customers, because there are many competing priorities when it comes to privacy. This is no different for the DHS Privacy Office.

The challenges that arise while implementing privacy at Nationwide became apparent immediately. In business, information is money. At Nationwide, the more a division knows about an individual, the better the company can protect the financial needs of the individual. However, certain laws or contractual obligations between parties often make it difficult to "know" everything about a customer. It is equally true in both the private and public sectors.

Let me give you an example of how this can impact a company:

> Susan works for a municipality and has a 457 deferred compensation plan with Nationwide that she obtained through her employer – a municipal government – whose relationship is with an independent producer under contract to Nationwide. Susan also has a Nationwide Insurance Agent through whom she purchased auto and homeowners insurance. Susan trusts her Agent to help her protect her financial assets – specifically, her house and her car. One day, Susan visits her agent and says that she has accepted a new job with a private company and is moving to a new city. Based on this scenario, one can see that Susan has at least three financial needs:
>
> 1. Change her auto insurance to a new state;
> 2. Change her homeowners insurance to the new state and residence;
> 3. Consider options for the assets in her 457 plan.
>
> Today, the Agent can help Susan with the first two of her three financial needs. It would help Susan the most if the Agent could also look up the details of her 457 plan and provide this information to a licensed Nationwide broker to help Susan understand options for getting the most out of her 457 plan after she moves to a new job. But, for a variety of legal reasons, the outcomes of privacy implementation at Nationwide prevent this from occurring. The Agent does not have access to – nor does he even have knowledge of – Susan's 457 plan information and, thus, he cannot help her consider options after she changes jobs.

I bring up this simple example to illustrate the challenges with implementing privacy. With every assessment, task to address a gap, or audit, there are three competing factors vying for the most beneficial outcome from their perspective. These include:

1. The business need for quick access to abundant amounts of personal information. Remember, information is money. The business cannot succeed without personal information.

2. The customer expectation. The customer wants the product or service that purchased or contracted for. The customer also has high expectations for how they want companies to manage and use their information. In short, they want it locked in a vault stronger than Fort Knox. But at the same time, they want Nationwide to be able to access it via phone, e-mail, Internet, or Agent

24 hours a day, seven days a week. They also expect to be provided additional products or services that can either save them or make them money. These are in and of themselves other competing interests for companies to manage.

3. The privacy regulations. Like all regulations, they serve a good purpose, in this case: protect individual investors or insured. But, they also come with unintended consequences, just like Susan's example from above.

As you can see, the job of a Privacy Officer is to help balance these three competing interests, like a carpenter of a three-legged stool. Picture a three-legged stool. The benefit of having three legs instead of four is that each leg can be a slightly different length, yet the stool will still function as a stool, even if it is a little lopsided. Because, in the end, it rarely happens that each leg of the stool – each of the three competing interests – is exactly equal. Generally, they are different. Sometimes, the privacy regulation is a bit longer, meaning the most important interest in a given business project. Other times, the interest of the customer or the business is given a slightly greater importance. But, the stool still functions as a stool.

This is no different for the DHS Office of Privacy. Ms. Cooney, her predecessor and those who will follow her, has also been asked to become a carpenter of a three-legged stool. But, in the DHS Privacy Office's case, the three competing interests are:

1. Government's responsibility for security, including responsibilities under the Homeland Security Act, the Aviation and Border Security Acts, and others
2. Individual privacy expectations;
3. The Privacy Office's responsibilities under Section 222 of the HAS, the Privacy Act, the Freedom of Information Act, and other competing and compatible privacy laws.

Listing the challenges that arise when implementing privacy is easy; resolving them takes time and resources and the power to effectuate the necessary change. It is a constant balancing act often with different outcomes each time an issue arises. It is hard to argue that the DHS Privacy Office is not faced with tremendous challenges in this area, as they balance the nation's collective security interests against the individual's interest in privacy.

A Very Brief Analysis of the DHS Privacy Office

Now, compare and contrast the process that I have just described to the DHS' Privacy Office: assess, address, audit, and repeat. All four steps must be tailored to government processes and then followed in the DHS for the Privacy Office to meet the requirements set forth by the Homeland Security Act, the Privacy Act, and several other laws regulating the government's use of personally identifiable data. Consider also the discussion about balancing important competing interests within an organization.

As you know, the Homeland Security Act (HSA) of 2002 authorized the formation of the Department of Homeland Security and the addition of a secretary to the president's cabinet to oversee the new department. Among other things, the Homeland Security Act also provides that the Secretary "shall appoint a senior official in the Department to assume primary responsibility for privacy policy, including:

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and

(5) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters."

To operationalize its legislative mandate, the DHS Privacy Office developed a Mission Statement that states tthe mission of the DHS privacy office is to minimize the impact on the individual's privacy, particularly the individual's personal information and dignity, while achieving the mission of the Department of Homeland Security." The mission goes on to state – and I am summarizing here – that the Privacy Office will achieve this goal through:

1. education and outreach efforts to infuse a culture of privacy across the department,
2. communicating with individuals impacted by DHS programs to learn more about the impact of DHS policies and programs, and,
3. Encouraging and demanding adherence to privacy laws.

Anyone who reads this Mission can see that the DHS Privacy Office is faced with the exactly same opportunities and challenges that any privacy office, including mine, faces every day – but on a much, much larger scale, and with a completely different risk dynamic. At Nationwide, my office is responsible for educating employees and establishing a culture of privacy, resolving the natural conflicts that occur with business interests in regard to this concept of privacy, and requiring adherence to privacy laws. There would appear to be little difference between my mission and the mission of the DHS Privacy Office.

Nevertheless, *one wonders whether the DHS Privacy Office has the budget, staff and institutional authority to adequately carry out its mission*. I will address some of these concerns in my recommendations and considerations below. In fact, the DHS Privacy Office has done a wonderful job working with the limited resources made available to it. They have done many of the assessments of existing DHS programs and appear to be integrated into the planning and review processes for future programs or programs under development. They have addressed most of the gaps discovered through their initial assessments. They also have a nascent employee privacy education component, although it lacks adequate funding. Where they could probably use the most assistance and resources is with operating their ongoing monitoring and audit function. This function is in its infancy and is inadequately staffed. Even if it were adequately staffed, it is doubtful that the Privacy Office has the legal authority to conduct the type of deep analysis necessary to ensure ongoing adherence to privacy laws. This incongruity is addressed further under my recommendations, below.

In sum, the Privacy Office is well organized and understandswhat it needs to do to carry out to meet its objectives. Its staff is highly motivated and experienced. However, they may lack support from the top and they clearly lack the financial resources necessary to effectively do the job Congress directed them to perform through Section 222 of the HSA.

Recommendations and Items for Consideration

While there are always risk assessments and balancing tests between privacy and other interests that must occur whether one is working in a public or private sector privacy capacity, there are still a few things that Congress should consider to make it more likely that our nation's privacy laws are not violated. Therefore, I respectfully submit the following for the Committee to consider as it defines its future agenda:

1. Strengthen the Statutory Authority of the DHS Privacy Office. The Privacy Office should have a clear and direct reporting line to Congress. If Congress is uncomfortable with Inspector General-like powers, then consider taking a half-measure and give the Privacy Office ombudsman-like power. Burying the office inside DHS means that it will never have the authority or respect it needs to carry out its mandate. The Privacy Office will rarely be able to act independently, and it will spend more time merely trying to survive politically than it will carrying out its mission to protect our citizens' privacy.

2. The DHS Privacy Office should have a larger budget to carry out its critical mission. The current $4.3 million budget does not on its face appear sufficient in light of DHS' overall budget to protect the privacy of all Americans. The difference between this year and last year's budget is only an increase of a few hundred dollars. I would doubt that any other area of DHS saw this paltry of an increase in its budget.

3. Congress should consider adding Chief Privacy Officers and Privacy Offices to all federal agencies, or at least those that generally collect and process personal information on citizens. Congress may even want to consider creating a Federal Data Commissioner, similar in authority and scope to those existing in the nations of the European Union. The Data Commissioner could either be the first among equals, or it could be the overarching policymaking body for enforcing all federal data processing. This body would have inspector general powers.

4. Transparency in information processing is fundamental to the role that the Privacy Office plays. The Freedom of Information Act Office needs to stay connected to the Privacy Office, because this is the Privacy Office's single real connection to its customers, namely U.S. citizens. One of the hallmarks of fair information practices is the ability of citizens or customers to know what information an entity has on them and have the ability to correct any erroneous information. This is simple due process and improves the integrity and accuracy of any organization's data. This role is naturally played the Privacy Office.

5. DHS should quickly appoint an official replacement for Nuala O'Connor Kelly, who left many months ago. The Acting Privacy Officer, Maureen Cooney, is doing a very capable job and should be seriously considered as the official replacement. However, the optics of not having an official replacement devalues the Privacy Office politically and organizationally. It indicates the job being capably performed by the staff may not be seen as worthy by senior department and administration officials as other areas in DHS and this undercuts the Privacy Office's authority.

Conclusion

I hope that my testimony helped illustrate the large effort, cost, and authority necessary for a corporation to effectively implement a privacy office. In order for the DHS Office of Privacy to effectively carryout its statute-defined requirements, it will need resources and the authority to implement a privacy program that balances the requirements of law, the responsibility of the government to protect its citizens, and the individual right of privacy.

Additionally, as I stated above, no privacy office can be successful without clear and strong support from the top. If support from the chief executive is absent, the privacy function will never be able to effectively carry out its mission. In fact, trying to perform a privacy function without senior management support may be worse than not doing anything with privacy, because it provides an illusion of privacy without the reality of having any.

Thank you for inviting me to speak with you this morning. I would be happy to answer any questions that you may have. I would also be more than happy to speak with you again or to work with you and your staff on any privacy issue.